REMARKS

I. General Remarks

Claims 9-11, 14-15, 18-23, and 25-30 are pending herein. By this Amendment, Claims 7-8, 12-13, 17, and 24 are canceled, without prejudice or disclaimer; Claims 9-11, 14-15, 21-22, and 25-27 are amended; and new Claim 30 is added.

Support for the claim amendments and new claims is found in the specification at, *inter alia*, paragraphs [0016]-[0019], [0021], [0043]-[0050], [0059]-[0065], [0074]-[0075], [0078]-[0079], [0090]; and in the Figures. No new matter is added by this Amendment.

The Applicant has disclosed an invention with three parts each novel ,useful and non-obvious. The parts include:

1) a new method to conceal negotiating positions by partial encryption of the statements in a negotiating position (Claims 18 – 22 and 30),

2) a new method to conceal numerical values contained within a statement of a negotiating position (Claims 14 and 15), and

3) a new method of negotiation over concealed negotiating positions through a blind agent (Claims 25, 28 and 29) where the agent compares concealed negotiating positions that are not exchanged directly by the parties in the negotiation and where the agent is blind because it cannot decrypt the partially encrypted negotiating positions.

By the above amendments, Applicant has rewritten all claims to define the invention as distinct from and patentable over prior art. The Applicant believes that he has made a full and appropriate response to the claim rejections in the Office Action and requests a reconsideration of the claims and a withdrawal of previous objections.

II. Remarks on Amendments to Claims

Claim 9: The amendment changes the verb “copy” with “copy in full” to follow more closely the language of the description of invention [0050] and preclude an interpretation as “copy in part”.

Claim 10: The amendment substitutes the definite verb "selects" to describe a step in the process.

Claim 11: The amendment rephrases this claim for clarity. Supplemental explanation may be found in [0026] of the Description of Invention.

Claim 14: This claim has been amended to read as an independent claim because the invention is applicable outside of the processes of the other claims. The introductory phrase of the amended claim is taken from the terminology of [0065] of the Description of Invention and the claim itself is based on [0079]. The term "linear mapping" has a conventional meaning that is illustrated in [0079] of the Description of Invention.

Claim 15: This claim has been amended to follow the Description of Invention closely and to tie this dependent claim to the independent claim 14 by mentioning the linear mapping function.

Claim 21: The amendment inserts the phrase "partially encrypted" to connect the claim more closely to the Description of Invention and to clarify the phrase "without decoding encrypted elements", a phrase that is referring to a characteristic of the partially encrypted sentences in the concealed negotiating position.

Claim 22: This dependent claim is amended to depend on Claim 21 rather than claim 29 because the intended limitation applies to the comparison of sentences in Claim 22, which depends in turn on Claim 29. Support for these series of claims is found in [0018], [0075], and [0090].

Claim 25: This independent claim defines the innovation of the broker as a blind agent. In order to describe the negotiation method in sufficient detail that it may be implemented from this disclosure, some protocol elements that are common to all computer-assisted negotiation have been mentioned. The innovation lies in the Applicant's process of negotiation set forth in the series of phrases in Claim 25. The amendments in this claim supply additional explanation from the Description of Invention to define the negotiation method without any possibility of misinterpretation.

Claim 26: This claim was discussed in the Interview with Examiner and the meaning of one-way encryption was fully discussed. In any case, the meaning is clearly

explained in public literature. To recapitulate: *a one-way encryption key is a text or byte-string applied as the key in a cryptographic hash function in order to accomplish an encryption that is one-way in the sense that it is not reversible even by one possessing the encryption key except by brute-force and wherein said one-way encryption key when used with a cryptographic hash function is variously known as a key, a nonce, or a salt.* The cryptographic functions are well known and the Applicant does not claim the functions as a discovery. Applicant claims their novel application to partially encrypt statements in a negotiation position. The claim has been amended to specifically state the improvement.

Claim 27: This claim was added following the Interview with Examiner because the Examiner pointed out that the specific properties of one-way encryption are not required for the claimed invention and that symmetric key encryption is a functionally acceptable alternative. Claim 27 is retained with an amendment similar to the amendment to Claim 26 to specifically state the improvement.

Claim 30: The negotiation method is especially effective when combined with partial encryption. In the original claims, the methods for partial encryption emerge from the claims almost as a parallel discussion. This method of presentation complicated the interpretation of the claims and reduced the visibility of the innovation present in this invention. Consequently, the method for partial encryption is now found in independent Claim 30. Claim 30 is written as required by PTO "Rules of Practice" Rule 75 (37 CFR 1.75) part e. with the effect that the phrases of the claim which are well-known facts are stated first and then the improvement is disclosed.

III. Summary of Remarks

A detailed, paragraph by paragraph, response to the Office Action follows below. Here we summarize the major points.

A) De Vries Straw-man Solution

Many statements in the Office Action rely on De Vries [¶0005] wherein De Vries very briefly describes a hypothetical solution wherein so-called "interests" are encrypted and sent to a broker. De Vries uses this solution as a straw-man to show its faults before offering his own solution. De Vries's description does not disclose the Applicant's invention because the broker in De Vries's straw-man is able to decrypt the "interests". De Vries clearly states in [¶0005] that "the host then decrypts only those interests that actually match" (emphasis added). De Vries's host can decrypt because it is in possession of the key; thus, the broker of De Vries's [¶0005] is not blind. In contrast consider the Applicant's disclosure: "wherein said broker does not possess the encryption key and is unable to decrypt the negotiating position", which appears in claim (25). De Vries [¶0005] does not disclose the Applicant's negotiation process and teaches away from the Applicant's invention.

B) De Vries in Combination with Nagel

The Examiner states that it is obvious to combine De Vries with Nagel. However, this combination fails to disclose any of the three parts of the Applicant's invention.

De Vries proposes a solution to some problems that are among the several problems solved by the Applicant's invention; however, De Vries does not disclose any of the three parts of the Applicant's solution. Let us consider De Vries with respect to each part.

1) a new method to conceal negotiating positions by partial encryption of the statements in a negotiating position.

De Vries discloses a "set of interests" which is explained to be a set of terms either text or numbers. De Vries describes a complete, not partial encryption of these sets of interests. Applicant, on the other hand, discloses a method wherein the negotiating position contains structured data or statements where "structured data

consists of data values organized in statements obeying a grammatical rule" (Claim 30); and Applicant discloses a partial encryption based on statement grammar "each statement of the negotiation position is partially encrypted by distinguishing the grammatical words and punctuation from the remaining text, by preserving grammatical words and punctuation in unencrypted form, and by encrypting each item of the remaining text" (Claim 30). Thus, De Vries does not disclose Part 1 of Applicant's invention.

2) a new method to conceal numerical values contained within a statement of a negotiating position (Claims 14 and 15),

De Vries describes the problem solved by Applicant's Claims 14 and 15 but De Vries does not disclose any solution to the problem. All of the systems described by De Vries, whether proposed or merely hypothetical, rely on the well-known result that identical values encrypt to identical encrypted values. De Vries may be forgetting the next part of this common knowledge; namely, unequal values encrypt to unequal values and no method exists to determine the numerical order of the original values given only their encrypted values. Thus there is no method in De Vries to ascertain if a value lies within a range of values given only the encrypted values of the ends of the range. Therefore, De Vries does not disclose Part 2 of Applicant's invention.

3) a new method of negotiation over concealed negotiating positions through a blind agent.

The Examiner concedes that De Vries does not disclose part 3 of Applicant's invention. Indeed, De Vries teaches in his Abstract: "such disclosure or non-disclosure of interests is accomplished in accordance with the present invention without the use of a third party". Thus, De Vries does not teach Part 3 of the Applicant's invention. Applicant's invention is superior to De Vries because it avoids the vulnerability of De Vries's proposal to Dictionary Attack. The Dictionary Attack problem is described in Appendix 3 below.

In the final analysis, De Vries teaches only that there exists a problem to be solved. Next, we consider whether Nagel has ideas that may disclose relevant information. Again, we divide the examination into three parts.

1) a new method to conceal negotiating positions by partial encryption of the statements in a negotiating position.

Nagel describes a method for "selective obscuration" of identity data. In his method, Nagel recommends encrypting sensitive identity information and leaving other information unencrypted. His method is conventional and well known. It is also known by experts in the field that this conventional method is weak and unsatisfactory for reasons explained in Appendix 3 *The Deficiencies of Anonymous Identity Resolution*.

The Examiner has labeled Nagel's method as "partial encryption", although Nagel does not use that term. Nagel's method is based on data sensitivity and does not disclose Applicant's method for partial encryption based on statement grammar and disclosed by Claim 30 of Applicant's invention.

2) a new method to conceal numerical values contained within a statement of a negotiating position (Claims 14 and 15),

Nagel does not disclose Part 2 of Applicant's invention. Nagel does not mention the subject.

3) a new method of negotiation over concealed negotiating positions through a blind agent.

Nagel describes a system in which a third-party intermediate regulates and administers two-way communication between two parties over an encrypted channel. Can Nagel's intermediary teach us anything about a blind agent performing negotiation? Consider the steps needed to convert Nagel's administrative intermediary to a blind agent broker:

1. The two-way communication between the two parties must be broken.

2. the two parties must be informed that they are no longer communicating and are now negotiating with the new goal being the selective exchange of data.

3. the intermediary must be provided with a method to negotiate over encrypted information.

4. the intermediary and the two parties must be provided with a protocol or sequence of steps that will result in a negotiation over concealed terms that does not allow to the intermediary to read either negotiation position and prevents the release of the full negotiation position to the opposite party.

In other words, we need to supply all of the disclosure of Applicant's invention in order to convert the intermediary of Nagel into part 3 of Applicant's invention. By any reasonable standard, there is no obvious path from Nagel's intermediary to Applicant's blind-agent broker.

Of the three parts of Applicant's invention, De Vries discloses no part and Nagel discloses no part. Given that neither contains applicable teaching, the two sources do not combine in any apparent way to disclose Applicant's invention.

C) Snapp in Combination with Others

Claims 14 and 15 disclose a method to conceal "numerical values and value ranges" using a "linear mapping". The meaning of "linear mapping" is obvious to anyone familiar with mathematics. A mapping written as f(x) is linear
only if f(x1 + x2) = f(x1) + f(x2). The algebraic expression for a linear mapping is a first order polynomial written f(x) = a + b * x; where a is the offset and b is the scaling factor. Snapp does not disclose a linear mapping.

Snapp discloses an address calculation method whereby "The offset circuit determines which bits in the bit array to turn on". He is explaining an address calculation for computing bit positions. His method is conventional in that it divides a bit address into two parts one of which is used for a word address and the other part of which is used with masking functions to find the proper bit within a word. This bit address

mapping is non-linear in its properties. Moreover, all bit-array addresses are integers whereas the variables of a linear mapping are real values (floating point in computer terminology). Because Nagel's subject is completely different from Claims 14 and 15, Snap does not use the concepts of "linear mapping", "secret offset", and "secret scaling" which are all necessary to the disclosure of Claims 14 and 15. In summary, Snapp does not disclose any information pertaining to the Applicant's invention.

D) Conclusion

The references cited in the Office Action do not disclose the methods of the current invention either separately or in combination. The Applicant requests a reconsideration of the claims as amended.

In the following remarks, we consider the paragraphs of the Office Action in detail.

III. Remarks on Rejections under 35 USC 112

Claims 7-10, 11-15, and 25-27 were rejected under 35 U.S.C. 112, second paragraph, as assertedly being indefinite. Applicant has amended claims to remove any quality of indefiniteness. Particular amendments are discussed in the following paragraphs. This rejection is respectfully traversed with respect to the pending claims.

Concerning Office Action Paragraph 9a)

The Examiner has interpreted the phrase in Claim (25) "the party who is asked to begin" as meaning "the party who is selected to begin". This interpretation is correct and the claim has been modified to use a consistent verb.

Concerning Office Action Paragraph 9b)

The Examiner states that the term "one-way encryption key" as used in Claims 8 and 26 is indefinite. For practitioners of the software arts or cryptography the term "one-way encryption key" has a definite and unambiguous meaning. A person with ordinary skills in these arts will understand that "one way encryption key" refers both to an entity (the key) and its associated cryptographic process (cryptographic hash function or CHF). Moreover, this term refers very specifically to this entity in its process context. As evidence for the state of general knowledge the Applicant will cite explanations freely available on-line in Wikipedia. The references that we cite were found by Internet search of the term "one-way encryption key" a step that is easily repeatable by any person with Internet access.

For example, the article available from URL http://en.wikipedia.org/wiki/Keyed-hash_message_authentication_code explains the application of a CHF written as HMAC(k, m) to encrypt a message text, m, with a key, k. Said encryption is irreversible and hence one-way. The article employs the words "key" or "secret key" where claims 8 and 26 employ "one-way encryption key". It would be obvious to one familiar with the standard cryptographic method that the meaning of this term implies a key used to accomplish one-way encryption via a CHF.

In a second example, the "one-way encryption key" is explained in the public article http://en.wikipedia.org/wiki/Cryptographic_hash_function and the application of said key in a CHF is illustrated in the first paragraph of the section titled Applications. Note however that this paragraph employs the term "nonce" rather than "key" because this word and the word "salt" are frequently substituted for the word "key" when it is desired to emphasize a different aspect of the CHF. For example see the typical sentence from this paragraph "Alice can prove that she had a solution earlier by revealing the nonce to Bob". Prior to this step, the nonce had been employed for a one-way encryption of the solution by a CHF. The Applicant would like to note that the

hypothetical parties Alice and Bob do not employ the services of a broker because the negotiation described in this public article is simpler than and serves a different useful purpose than the claimed Invention.

The Applicant has shown that the term "one-way encryption key" has a meaning that is well understood by an average practitioner in this field; therefore, the term has a definite meaning for one skilled in the art of encryption.

In addition, the Applicant notes in connection with this rejection that the subject of one-way encryption was discussed in the Interview with the Examiner of December 2007 and that Applicant thereafter modified the structure of the claims appropriately with the exception of claim (8). On further reflection, the applicant withdraws claim (8).

Concerning Office Action Paragraph 9c.

Claim 8 is cancelled.

Concerning Office Action Paragraph 9d.

The Office Action quotes claim (9) as reading "wherein both parties never receive a copy of the opposite party's negotiation". The reason provided for the objection is that the word "copy" might be interpreted by someone to read "copy in part" rather than intended meaning of "copy in full". Claim 9 has been amended to read as intended.

Concerning Office Action Paragraph 9e.

The Office Action rejects claim (11) based on the relative nature of the auxiliary verb "may" which does not suggest a positive step in the negotiating process The Applicant agrees that the phrasing of the claim implies but does not explicitly state a positive step. Claim (11) has been amended to recite a positive step.

Concerning Office Action Paragraph 9f.

The Office Action rejects claim (10) because the phrase "has the opportunity" does not express a positive step in the negotiating process The Applicant has amended claim (10) to recite a positive step in definite terminology.

IV. Remarks on Rejections under 35 USC 103

Claims 8-13, 17, 19-23, 25, 28 and 29 were rejected under 35 U.S.C. 103(a) as being obvious. This rejection is respectfully traversed.

Concerning Office Action Paragraph 11.

The Office Action rejects claims 8-13, 17, 19-23, 25,28, and 29 under 35 U.S.C. 102(b) citing the publication of De Vries and the patent of Nagel. De Vries proposes a totally different invention as is apparent immediately from De Vries''s Abstract where he states: "such disclosure or non-disclosure of interests is accomplished in accordance with the present invention without the use of a third party". Thus, De Vries fails to disclose the "blind agent" broker that is key advance of the Applicant's invention.

De Vries employs one-way encryption with a cryptographic hash function – an idea that is found in textbooks and that is also incorporated in the Applicant's invention. However this standard teaching is insufficient to prevent a Dictionary Attack as discussed in Appendix 3: *De Vries and Similar Proposals Are Vulnerable to Dictionary Attack*. To prevent such attack, a blind-agent broker as disclosed by the Applicant is essential.

Nagel describes a workable invention for two parties to communicate using encryption methods following a method administered by an intermediary. Nagel's invention sends information in full and intact from one party to another. The intermediary

is outside the communication channel. Thus Nagel's invention fails to instruct in the process necessary to conduct a negotiation over concealed terms through an agent and thus fails to disclose the Applicant's invention.

For a full discussion of these points, please see the remarks above in "III. Summary or Remarks, B) De Vries in Combination with Nagel". We repeat here only the conclusion:

Of the three parts of Applicant's invention, De Vries discloses no part and Nagel discloses no part. Given that neither contains applicable teaching, the two sources do not combine in any apparent way to disclose Applicant's invention.

Concerning Office Action Paragraph 12a)

The Office Action states that paragraph [¶0007] of De Vries discloses "conducting a negotiation between parties through a broker". In fact, this paragraph makes no mention of brokered negotiation as claimed in the Applicant's Invention. De Vries states without qualification "this scheme does not require a trusted third party or host at the time potential matches are made". The current invention requires a trusted third party namely the broker agent; therefore, The teaching of De Vries fails does not correspond to the language of the Applicant's claim; it fails to disclose Applicant's Invention; moreover, it instructs the reader in an entirely different direction.

Concerning Office Action Paragaph 12b)

The Office Action references De Vries relating to the phrase "wherein each party receives from the broker a dictionary of words for description of its negotiating positions". This phrase appears in Claim (25) of the current Invention, which is an independent claim that describes the novel invention -- a method of negotiating agreement over concealed terms through a blind agent. To serve as an effective claim, it must be possible for a software practitioner of average talent to implement the claimed

invention. This phrase in claim (25) provides guidance to allow implementation of the invention. This phrase within claim (25) should not be construed as a standalone claim.

Regarding the reference to paragraph [¶0004] in De Vries that is cited in Office Action 12b), the Applicant would like to call attention to the paragraph itself which begins "By way of background, one conventional scheme…" and ends with "Consequently, the device does not provide a capability for privacy or non-disclosure…". De Vries uses this paragraph to describe a very unsatisfactory and useless alternative to De Vries's device. The text of De Vries [¶004] contradicts the claims of the Applicant's invention. The purpose of paragraph [¶0004] is to establish a context of poor practice as a motivation for future inventions. Hence De Vries paragraph [¶0004] does not disclose the invention.

Regarding the reference to paragraph [¶0044] in De Vries that is cited in Office Action 12b), the Applicant would like to call attention to the paragraph itself which states "In a preferred embodiment, it is assumed that a hash sequence used for encoding interests is known to all entities exchanging shared interests." This statement illustrates that De Vries lacks a concern for dictionary attacks. In contrast, the broker in the current invention does not possess the hash sequence (one-way encryption key). Moreover, each key in the current Invention is used only by the two parties and only for that session. Only the author of each negotiating position and the broker can possess an encrypted negotiating position but the broker is prevented from launching a dictionary attack against the encrypted position because the current Invention does not allow the broker to have the key. Applicant's invention is a major improvement over the device proposed by De Vries owing to the addition of the Applicant's blind-agent broker and the negotiation method disclosed in Claim (25).

The Examiner reads the phrase "set of interests" in De Vries as being comparable to the term "schema" in the Applicant's claim. This is clearly not a valid comparison. De Vries's teaching makes clear that a "set of interests" is a set of words or

symbols equivalent in computer languages to a set of values of an enumeration or in user-interface design to a multiple choice option list. In the Applicant's invention, a negotiation is expressed as sentences following a syntax rule. In one embodiment, the sentences are specialized to XML statements expressed in an XML schema. Two different concepts are involved in the phrases "set" and "schema" and this would be evident to anyone skilled in the art of representing information for computer purposes.

Concerning Office Actions Paragraphs 12c) and 12d):

The overall theme of the objections in these paragraphs of the Office Action is that previously known mechanisms use encryption, the current mechanism uses encryption and therefore the current mechanism is not patentable over prior art. Such an objection is equivalent to examining a mechanical device, finding gears, levers and springs and then searching prior art to find devices that contain gears, levers and springs. By law, however, a new mechanical device is patentable if the combination of gears, levers and springs in the new device is novel, non-obvious and useful. Likewise we see in the current invention a combination that includes known components such as encryption, XML and secure network communication. A search of the literature shows that the Applicant's combination is not disclosed in any earlier art. Moreover, the result is highly useful and may even possess decisive advantages for national security applications. In spite of indications that the Applicant's Invention is a valuable advance, other inventors have not found it. That fact alone argues that the Applicant's invention is non-obvious.

The Applicant would like to request that all objections to the invention based on the principle that some components of the invention were used in other mechanisms should be withdrawn in the face of evidence that the current invention is novel, non-obvious and useful. In the following, Applicant addresses individual subparagraphs in their particularity.

Concerning Office Action Paragraph 12c)

The Office Action says that the statement in Claim 25 "wherein the party who is asked to begin negotiation sends an encryption key to the other party" as obvious from the statement "communication between parties is encrypted using a conventional key" (emphasis added). Read in context, we see the uniqueness of the current invention because the key exchange explained in this phrase of claim 25 is never used to communicate between parties. It is used as part of the negotiation protocol to prevent the broker from interpreting the partially encrypted negotiation positions. Thus the language of the claim and the invention are distinct from prior art and non-obvious.

Concerning Office Action Paragraph 12d)

The examiner points out that the phrase "identical terms encrypt to identical values" is well-known. As discussed above, this and other well-known properties of encryption systems are employed in the current invention in a novel and useful combination that is not obvious. In particular observe the phrase in full: phrase "each party applies the encryption key to partially encrypt its negotiating position so that identical terms encrypt to identical values" (emphasis added). Note that the well-known encryption occurs within Applicant's invention of "partial encryption" disclosed for the first time by the Applicant and it is used with Applicant's innovative and non-obvious negotiation process. The use of known cryptographic techniques in the Applicant's partial encryption and negotiation inventions is not obvious from the prior art.

Let us consider whether the cited references to prior art are relevant to the claims of the current invention.

De Vries in paragraph [¶0014] provides an excellent problem statement. It fails as a prior art reference because De Vries fails to disclose a satisfactory method to solve the problem as stated in [¶0014]. The current invention offers a novel and satisfactory solution that meets De Vries stated goal and other more advanced goals.

For example, De Vries [¶0014] states "the only interests of the seller that are disclosed to the buyer are those objects in the seller's inventory that the seller is willing to sell for a price acceptable to the buyer". However, compare this statement to the mechanisms described by De Vries. If limited to these mechanisms, a seller might ask $3.99 and a buyer might offer $4.00; but, since these two numbers encrypt to entirely distinct hash values, there is no match even though buyer offered more than seller asked! Although De Vries fails to disclose a mechanism suitable for negotiating price, the current invention does so. For example, the seller might ask $3.50 to $1000, a range from the lowest acceptable price to the maximum, dream profit point. The buyer might offer $1.00 to $4.10, a range from a fire-sale low point to the buyer's pain threshold. With the mechanisms of this invention, the broker finds a compromise price that when revealed will be acceptable to both, for example $4.05. De Vries offers no method to achieve this useful outcome; the Applicant's invention discloses an effective solution.

Lastly and most importantly, De Vries sets the standard too low in his problem statement. De Vries does not secure his system against dictionary attacks against his encrypted interest lists. De Vries envisions an unnamed entity operating an interest matching machine. In his account of his proposed mechanism, he clearly indicates that the machine is operated by the participants. For example in De Vries SUMMARY OF INVENTION [¶0009], he states unequivocally that "such matching is accomplished without the use of an intermediary application, scheme, or process". Consider now the effect of De Vries proposed solution. Each "entity" as defined by De Vries broadcasts encrypted interest lists to other entities who then compare said encrypted interests with their own encrypted list by means of the mechanism shown in De Vries Figure 1. In the final analysis this accomplishes nothing more than an encrypted communication channel that fully and faithfully transmits one entity's interest list in full and entire to another entity. The list may be encrypted but the recipient has the key. The encryption algorithm may be one-way, but the recipient can break one-way encryption by encrypting the dictionary of interests and using the resulting code pairs to decode the

encrypted by matching encrypted interests with the complete list of code pairs. This is an example of dictionary attack (see Appendix 3).

We see than that the Applicant's Invention effectively provides a disclosure of matching interests and a concealment of all others whereas De Vries instructs us to omit the intermediary leaving the information vulnerable to disclosure.

In the final analysis, De Vries's proposed methods are inadequate even for the problem he sets for himself. The methods he discloses are inadequate to instruct a person in the proper solution to the problem. The current invention is patentable over De Vries's attempted solution because De Vries failed to find a satisfactory solution and he teaches away from the proper solution which is the blind agent found in the current invention. The current invention is a major improvement because it uses a blind-agent broker who cannot direct a dictionary attack against the negotiation positions because the broker does not posses the one-way encryption key.

Concerning Office Action Paragraphs 12 e) and f):

In these paragraphs of the Office Action, the Examiner juxtaposes a phrase extracted from Claim (25) with De Vries paragraph [¶0005]. The purpose of these juxtapositions is unclear because this paragraph in De Vries clearly shows his teaching does not disclose the method of claim (25). In fact, De Vries teaches away from the method of claim (25) because De Vries clearly states in [¶0005] that "the host then decrypts only those interests that actually match" (emphasis added). De Vries's host can decrypt because it is in possession of the key, a fact that contradicts the method specified in claim (25). The method reported by De Vries in [¶0005] is clearly inferior to the current invention because nothing prevents the host from decrypting all of the interests. We should also note again that De Vries set of "interests" is merely a set of keywords: a simple mechanism that fails to disclose the current invention, which uses partially encrypted statements.

In Office Action Paragraph 12e) the Examiner juxtaposes De Vries paragraph [¶0005] with the phrase "wherein each party sends its partially encrypted negotiating position to the broker". It is apparent that this association is unjustified because the third party intermediary discussed in [¶0005] does not possess an understanding of partial encryption as specified in the current Invention. Moreover the third party intermediary in [¶0005] can decrypt interests whereas the blind-agent of the current invention cannot decrypt the partial encryption; therefore De Vries's third party intermediary in [¶005] is not equivalent or comparable to the broker specified in the current invention.

In Office Action Paragraph 12f) the Examiner juxtaposes De Vries paragraph [¶0005] with the phrase "wherein said broker does not possess the encryption key and is unable to decrypt the negotiating position" which appears in claim (25). It is apparent that this association is unjustified because the third party intermediary discussed in [¶0005] is said to be able to decrypt the interests thus demonstrating without possibility of misinterpretation that the third party of De Vries is in possession of the encryption key in contradiction to claim (25).

Concerning Office Action Paragraphs 12g

The Examiner cites De Vries [¶0011] wherein De Vries recites the commonplace knowledge that encryption is a deterministic process with the effect that identical strings will encrypt to identical values and therefore encrypted values may be reliably compared to establish whether or not the original strings are identical. On the other hand, De Vries does not disclose the method of partial encryption nor the existence of the broker in the current invention specifying in [¶0010] of his SUMMARY OF INVENTION "such disclosure or non-disclosure of interests is accomplished in accordance with the present invention without the use of a third party" and repeating this specification for emphasis in his DETAILED DESCRIPTION [¶0042]. Moreover, De Vries explains in [¶0011] and elsewhere in his specification that a set of interests is a set of values represented by a

string of variable length with minimum of one bit. Such a set of interests has limited descriptive power and cannot be reasonably compared to the statements used in the negotiation positions for the current Invention.

The teaching of De Vries lacks the "blind agent" broker and "partial encyption" and "statements of negotiating position" that are essential to the current invention therefore it is impossible to infer Applicant's invention from De Vries.

Concerning Office Action Paragraphs 12h

The Examiner draws attention to a phrase in De Vries [¶0004] which we repeat here in its context with the Examiner's phrase underlined: "By way of background, … Where an automatic comparison of interests of the receiving device and the broadcasting device indicate that there is a shared or common interest, an audible or visual alert is provided by each device…". The Applicant draws attention to the fact that the "device" in question is hypothetical and is invoked by De Vries to point out a deficiency, namely, that such device lacks encryption. Such a hypothetical device shows a further deficiency with respect to the current invention because it does not use a blind-agent broker.

The Applicant has described an invention with a blind-agent broker that operates on partially encrypted statements. The Applicant has not claimed a method involving a bell or visual signal and there is no place for either device in the Applicant's design. No part of De Vries [¶0004] discloses any of the three parts of the Applicant's invention.

Concerning Office Action Paragraph 12i

The Examiner considers the phrase contained in Claim (25) "wherein the broker provides the parties with a copy of an encrypted basis for agreement" in the light of the teaching of De Vries. However it is clear from the preceding discussion that the teaching of De Vries is inferior in utility to the current invention and that De Vries directs the

reader away from an understanding of the current invention. As mentioned before, De Vries does not believe a broker should be used; therefore, the phrase in claim (25) "wherein the broker provides" finds no corresponding step in De Vries where no broker exists. The phrase "encrypted basis of agreement" in claim (25) clearly refers to the partially encrypted statements of the negotiation positions whereas the phrase "match interests" in De Vries clearly refers to his functionally inferior method of representing interests by a set of discrete values. There is no obvious path from the teaching of De Vries to the claims of the Applicant's invention.

The cited paragraph [¶0047] in De Vries discusses a partial matching process. Applicant has made no claim about a partial matching process. De Vries does not disclose the Applicant's claims and Applicant does not claim a partial matching process.

Concerning Office Action Paragraph 12j

The Office Action cites De Vries paragraph [¶0047] in juxtaposition with a phrase from claim 25: "wherein each party decodes the basis-for-agreement". De Vries points out in paragraph [¶0047] "In a further embodiment, a communication channel between the entities engaged in comparison of interests is itself encrypted using conventional techniques .... and is useful for preventing unauthorized third parties from acquiring useful information". Plainly and simply, De Vries is explaining well-known encrypted communication in an obvious manner that does not pertain to claim (25). In fact, De Vries in this paragraph as in other places in his proposed solution instructs the reader to allow free comparison of interests, which is a far cry from the negotiation in the current invention. In regard to the claim language, please note that the party receives the basis-for-agreement from the broker but there is no broker in De Vries's system; moreover, the basis-for-agreement contains partially encrypted statements whereas there are no statements in De Vries and certainly no partial encryption; therefore, De Vries does disclose the claim language.

The Applicant notes that the cited paragraph [¶0047] in De Vries corresponds directly to a phrase in claim (28). Anticipating that Examiner may have intended claim (28) rather than claim (25), Applicant points out the structure of claim (28) in the relevant phrases: "wherein public key encryption protects information exchanges so that only an intended recipient can decrypt the information and authenticate the sender, wherein the improvement comprises: " (emphasis added). The general knowledge recited in claim (28) does indeed match the general knowledge recited in De Vries [¶0047]; however, claim (28) clearly designates such general knowledge as being distinct from the improvement disclosed in the claim. Claim (28) was cast in its current form in response to commentary in the Interview with Examiner to meet Examiner's desire to see the improvement of the current invention clearly distinguished from prior art and general knowledge. Consequently, claim (28) is crafted as required by PTO "Rules of Practice" Rule 75 (37 CFR 1.75) part e. The phrase which corresponds to information in De Vries is clearly placed in part 1 of the claim - the preamble - and the line demarking the boundary between prior knowledge and invention is established by the phrase "wherein the improvement comprises".

Concerning Office Action Paragraph 13:

In this paragraph the Examiner argues that the teachings of De Vries and Nagel can be combined to derive the current invention; in addition, the Examiner argues that such a combination "would have been obvious to a person having ordinary skill". Upon closer reading of Nagel's patent publication; it is clear that the issue of skill is irrelevant because De Vries and Nagel, even in combination, no do not instruct in the construction of the current invention. The inadequacy of De Vries's approach to the problem was discussed above. In the following we discuss Nagel.

Nagel's invention is applicable in the field of secure two-party communication whereas the current invention is a method of negotiating wherein a third-party receives concealed negotiating positions and finds matches within the positions. The conceptual

difference between two party communication (Nagel) and matching concealed information via a broker (Applicant's invention) is sufficiently great to preclude any person from applying Nagel's methods to a brokered information matching method.

The Office Action states "Nagel discloses an intermediary, wherein the intermediary is unable to decrypt the communication". Nagel writes of this intermediary that it is "outside the direct communication channel". Because Nagel's intermediary is outside the encrypted two-way communication channel, it is obvious that the intermediary plays no role in the two-way communication. If the intermediary attempts to eavesdrop on the two-way communication, the intermediary finds it is encrypted; therefore, the intermediary cannot decrypt it. When Nagel writes that the intermediary "never possesses sufficient information to intercept and decrypt the communication" he only states the obvious purpose of the encrypted two-way communication channel.

Nagel does not disclose "wherein each party sends its partially encrypted negotiating position to the broker"; Nagel's intermediary does not receive the communication. Nagel does not disclose "wherein, upon receiving both partially encrypted negotiation positions, the broker compares them to discover whether there exist encrypted statements that are common with both negotiating positions". On the contrary, Nagel's intermediary receives nothing, compares nothing, and is not acting as a broker for a negotiation. Thus Nagel has made no disclosure that can be combined with De Vries to infer the Applicant's invention.

The Examiner points out that Nagel recommends in column 17 lines 3-27 "only the personally identifying information needs to be obscured". Nagel's suggestion to encrypt "personally identifying" data and not other data fails to disclose the partial encryption method disclosed by the Applicant. Nagel proposes an entirely different method than the Applicant's and a person reading Nagel would be lead in a different direction than the current invention. Lastly, we must note that Nagel's suggestion is

commonplace and leads to well known problems that are described below in Appendix 1 *The Deficiencies of Anonymous Identity Resolution*.

Concerning Office Action Paragraph 14:

The Applicant notes that Claims 26 and 27 have been amended in this response and Claim 8 has been cancelled. Claims (26) and (27) have each been amended to show their connection with the independent Claim (25) and to separate Applicant's invention from prior art in the manner prescribed by PTO "Rules of Practice" Rule 75 (37 CFR 1.75) part e.

Concerning Office Action Paragraph 15:

Office Action Paragraph 15 cites paragraph [¶0006] in De Vries. De Vries [¶0006] is a continuation of a discussion of a hypothetical scheme that began in De Vries [¶0005]. De Vries's hypothetical scheme instructs the reader in an incorrect and unsatisfactory method for reasons already explained above in the paragraphs under the heading "Office Actions Paragraph 12 e) and f)". We reference the reasons stated above demonstrating that De Vries's teaching is misleading and prevents rather than enables a person to understand the current Invention.

We note specifically that De Vries does not disclose the claim language "wherein both parties never receive a full copy of the opposite party's negotiation position" because the method of "negotiation position" as disclosed with Applicant's invention is different from De Vries set of interests. Note in addition that in De Vries's proposed system (not the hypothetical system of [¶0005]-[¶0006]) the parties actually receive an encrypted copy of each other's set of interests and that each party in De Vries's proposed system does in fact have the capability to decrypt the set of interests. (See Appendix 3)

The paragraph [¶0009] in De Vries cited in Office Action Paragraph 15 is the beginning paragraph of his SUMMARY OF INVENTION wherein De Vries states the problem purportedly solved by his proposed mechanism. De Vries believes he is able to match interests "without the use of an intermediary application, scheme, or process" and "non matched interests are not disclosed". As we have described above, De Vries is incorrect in his belief; in fact, all interests are easily disclosed in this method due to his misunderstanding. The third-party blind-agent broker of Applicant's invention solves the problem stated but left unsolved by De Vries and Applicant's invention is clearly patentable over the teaching of De Vries.

Concerning Office Action Paragraphs 16 and 17:

In these two paragraphs, the Examiner juxtaposes De Vries [¶0016] with Claims (10) and (11) of the current invention. The Applicant can find no text in De Vries [¶0016] that relates in any way to Claim (10) or Claim (11).

In regard to Claims 10 and 11, the Applicant notes that De Vries is very specific in his teaching that each entity should broadcast the entity's interest set to all other entities for comparison by the entities and not by an intermediary. For example see De Vries [¶0060] wherein De Vries describes the operation as "each interest is disclosed to the other entities for comparison with those entities interest sets" (sic). This textual explanation is consistent with the graphical representation of De Vries's Figure 2 which clearly shows each entity communicating by broadcast with every other entity with no opportunity to select partners or to modify the interest set in the context of a specific partner. By teaching that the broker is unnecessary and teaching that all pairs of entities are forced into comparisons using a uniform set of interests, De Vries teaches in a direction remarkably different in direction from the current invention. Moreover, the fact that De Vries's proposed mechanism forces automatic comparisons is actually the opposite of negotiation. Negotiation is a voluntary activity controlled by each party in the

negotiation. No person could deduce the current invention from the teaching of De Vries.

In consideration of the fact that the statements of Claim (10) and Claim (11) are not disclosed in De Vries and in consideration that De Vries teaches away from the methods of these claims, the Applicant asks that the objections to Claim (10) and Claim (11) be withdrawn.

Concerning Office Action Paragraph 18:

Claim (12) is canceled.

Concerning Office Action Paragraph 19:

The Examiner repeats the objection of Office Action Paragraph 12f in the context of Claim (13). As discussed above, the objection to Claim (25) in the context of De Vries [¶0005] is unjustified because De Vries explicitly contradicts the method shown in Claim (25) and therefore teaches away from the discoveries of the current Invention.

Specifically, the claim reads "wherein the broker is unable to decrypt the basis-for-agreement" whereas De Vries [¶0005] states "where a match is identified, does the trusted host decrypt the interests" and later "host decrypts only those interests". De Vries's statements contradict rather than disclose the current invention. The claim says "unable to decrypt" while De Vries says "decrypts".

Claim (25) notes the broker cannot decrypt either negotiation position. In fact, lacking a key, the broker cannot decrypt any statement in either negotiation position. Claim (13) notes that the basis-for-agreement contains encrypted statements from the negotiating positions and therefore the broker cannot decrypt the basis for agreement

In view of the fact that the limitation of Claim (13) is already present in Claim (25) and in consideration that said limitation is essential to distinguish the Applicant's Invention from prior art and to explain the utility of the Invention, Claim (13) may be regarded as an unnecessary addition to the independent Claim (25). Consequently, Claim (13) has been withdrawn and Claim (25) has been modified to state explicitly the utilitarian consequences of the method disclosed in Claim (25).

Concerning Office Action Paragraph 20:

Claim (17) is cancelled.

Concerning Office Action Paragraph 21:

In regard to Claims 19, 20, 21 and 29, De Vries does not disclose any of the three parts of the Applicant's invention . Refer to the above discussion for details.

As discussed above, Nagel describes the selective obscuration of "personally identifying" information but does not disclose the Applicant's method of partial encryption. Hence, the Applicant's invention is patentable over Nagel in view of its novel partial encryption method and its superior utility.

Because all three essential parts of Applicant's invention are absent in De Vries and absent in Nagel, there is no obvious way to combine the two teachings and infer a useful result.

Concerning Office Action Paragraph 22:

As discussed above, De Vries does not disclose the methods of the current invention as demonstrated by the references to De Vries cited above. Note in particular that De Vries does not disclose "wherein the broker compares sentences in the

negotiation positions" because De Vries does not have a "broker" and De Vries does not have "sentences in a negotiation position".

Concerning Office Action Paragraph 23:

The Examiner cites De Vries [¶0013] in connection with Claim (23). The commonality between De Vries [¶0013] and Claim (23) lies only in the similarity of phrases in both texts recommending each method to the purpose of comparing prices. The application area is obvious in both cases. De Vries offers one method but it suffers two major problems. It does not provide adequate security for the information and it is unworkable because De Vries provides no method to compare encrypted price ranges. In contrast, the invention of the Applicant provides security thorough a novel and innovative negotiation protocol. Applicant also disclose through his invention, a method to conceal numerical ranges (e.g. price ranges) and successfully compare the concealed ranges during the negotiation process. De Vries recites only one application of the current invention but does not teach the art needed to replicate the current Invention; consequently, the objection is not substantiated by De Vries [¶0013].

Concerning Office Action Paragraph 24:

The Examiner cites De Vries [¶0015] in connection with Claim (23). In De Vries [¶0015] De Vries appears to be speculating that a well-know application usually called "subscription based messaging" could be improved by allowing De Vries's "interests" to serve as the selection criteria for a subscription. The Applicant is unable to find text in De Vries [¶0015] that pertains to Claim (23) and respectfully requests that the objection should be withdrawn with respect to Claim (23).

The applicant notes in connection with Office Action Paragraph 24 that claim (24) has been cancelled.

Concerning Office Action Paragraph 25:

As discussed above and shown by detailed citations to the text, Claim (25) is patentable over a combination of De Vries and Nagel because neither instructs in the art needed to discover the invention; De Vries teaches away from Applicant's invention, and Nagel is describing an unrelated subject.

Claims (7) and (18) show non-obvious limitations on Claim (25) that are not disclosed by prior art. Applicant notes that Claim (7) is herein withdrawn and replaced by Claim (30) wherein the Applicant explicitly distinguishes prior art from the current invention.

The Examiner claims the Applicant has made an Admission on this subject. That claim is incorrect. In the Interview with Examiner, Applicant made clear that markup language and XML in particular are prior art but that the use of these together with the Applicant's method of partial encryption disclosed in the current Invention is novel, useful and patentable.

During the Examiner Interview, the Applicant devoted considerable effort to explaining the unique and new invention. The invention is also clearly and precisely described by the claims. The claims disclose a new method of negotiation, a new method of partial encryption of statements in a negotiation position, and a new method for concealing numerical ranges in statements. The Applicant requests that the patent application be evaluated on the basis of these novel contributions to the state of the art as set forth in the claims. In consideration of these claims as amended, the Applicant respectfully requests the rejections be withdrawn.

Concerning Office Action Paragraph 26:

This paragraph of the Office Action continues the subject of paragraph 25. Applicant's remarks on paragraph 25 are also applicable to paragraph 26.

The Examiner states "Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the combination's teachings to include XML to allow users to create their own customized tags, enabling the definition, transmission, validation and interpretation of data between applications and between organizations." The Applicant would like to point out that "the definition, transmission, validation and interpretation of data between applications" are the textbook functions of XML. The Applicant has never claimed to invent XML or any of the standard applications mentioned by the Exxaminer. The Applicant teaches the use of XML in conjunction with the Applicant's method of partial encryption that enhances a novel process for negotiation over concealed negotiation positions. Both innovations are disclosed for the first time in the current Invention. The Applicant's invention of partially encrypted XML is a novel and useful improvement over unencrypted XML for the purpose of negotiation over concealed negotiating positions. .

As discussed above, the combination of De Vries and Nagel does not resemble the current invention and is inferior to the current invention. The Applicant requests that the invention be evaluated on its own claims and such evaluation will show it is patentable over any combination of De Vries and Nagel.

Concerning Office Action Paragraphs 27 and 28:

These paragraphs of the Office Action apply to Claim 14 and Claim 15. Claim 14 discloses a method whereby numerical values and value ranges may be concealed while preserving the comparison properties of a numerical value or value range

respectively. The question is whether this useful improvement has been taught or suggested before the Applicant's invention.

De Vries claims a method for encoding numerical value ranges (see De Vries [¶0013] but does not explain how it operates. By omitting an explanation of the mechanism, De Vries implies that it operates by virtue of comparing lists of interests because that is the subject of his proposal. Snapp does not claim or explain a method for encoding numerical value ranges.

Thus, the references to De Vries, Nagel and Snapp provide no support for the statement in Office Action Paragraph 27. The fact that the statement was made indicates confusion about the capabilities of De Vries's set of interests. A set of interests cannot implement a value range efficiently and even if it did, the Applicant's invention is clearly of a different nature. This point is discussed in more detail below in Appendix 2) *Sets of Interests Cannot Represent Value Ranges*.

Claim (14) requires the use of secret offset and secret scaling factor to be applied in a linear mapping of numerical values. We note that the method of numerical value concealment is an improvement that can be combined with the partial encryption used in the negotiation. If a statement in a negotiation position contains two numerical ranges, the question arises: how should the implementer select the secret scale and offset to optimize the concealment. Claim (15) answers this question. It would be obvious to anyone versed in the art of statistical data mining that, if the secret scale and offset are constant within the statement, the mechanism of Claim (14) might allow inferences on the relationship of different values contained in the same statement in an encrypted negotiation position. On the other hand, if each numerical value in a statement is concealed with a different secret offset and secret scale factor, then numerical relationships within each statement are also concealed. Thus for optimal security, we want to apply different scale factors in the same statement. In the context of the negotiation process, however, each party in the negotiation must apply the same

offset and scaling; otherwise the blind-agent broker cannot compare the concealed ranges. Claim (15) describes a method for deriving a different secret offset and scaling factor for each named value. In the context of Claim (14) this is a useful limitation on the method.

When Claim (15) is applied in the context of Claim (14) and Claim (25) we see that two the parties in a negotiation have agreed upon a single unique encryption key, which they employ to partially encrypt their negotiation positions. Being in possession of the same key, the parties are then able to derive a secret numerical scale and secret numerical offset that are different for each value in a statement. However, for each named value, both parties derive the same linear mapping.

The Examiner cites Snapp column 6 lines 33-53 in connection with Claim (15). The applicant notes that Snapp is describing a process of turning on bits in an array. Snapp starts with one address of 32 bits but he plainly is using the 32-bit value as a "bit-address". No modern machine is bit addressable. Instead, "bit-addresses" are always implemented in modern hardware by dividing the address represented by a bit string into a word address into storage and a bit address within each word. The hardware accepts the word address and the bit may then be set within the word by a masking operation. Thus, Snapp is simply stating obvious knowledge concerning the method of addressing a bit array on byte or word addressable hardware. Specifically Claim 15 says "the offset and the scaling factor" which are used in the context of independent Claim 14 in the "linear mapping". No language in Snapp discloses or uses the concepts of "scaling factor" or "linear mapping". Claim 14 and 15 use "offset" in the sense of numerical value offset in a linear mapping whereas Snapp uses "offset" in the sense of an address or array position offset in hardware.

VI. CONCLUSION

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

/Warren Zitlau/

Warren A. Zitlau, Esq.
Registration No. 39,085

CAHN & SAMUELS, LLP
1100 17th Street, NW, Suite 401
Washington, DC 20036

Telephone: (202) 331-8777
Facsimile: (202) 331-3838

Date: July 18, 2008

Appendices

The following sections consider certain topics in detail. They are referenced from the preceding remarks and may be read only as necessary for additional explanation.

Appendix 1: The Deficiencies of Anonymous Identity Resolution

Many reputable sources, including the Nagel patent cited in the Office Action, advocate the selective obscuration of identity information to protect privacy and secure sensitive data. These recommendations lead to anonymous data and matching by "Anonymous Identity Resolution", to borrow a phrase from IBM Inc. The method is incorporated in systems like AOL and Google where data on Internet users and their searches have been "anonymized" to protect the privacy of individuals.

Unfortunately, Anonymous Identity Resolution is deficient with respect to common sense requirements. Millions of people are involved and are at risk. To bring the problem to the public's attention, the New York Times ran a front-page article August 9, 2006 entitled "A Face is Exposed for AOL Searcher No. 441779". The person behind the face, Thelma Arnold, was not pleased to learn she had been randomly selected to have her name, residence, and buying habits made public so easily. The novel method of partial encryption disclosed in the current Invention is a vast improvement over prior art because it provides a more secure but still effective way to share protected data.

The following example follows Nagel's recommended partial encryption and shows step by step how it can fail to secure the data. This example illustrates why the system is insecure using a situation of personal interest to the Applicant.

Suppose a person suffers a myocardial infarction at home and is transported by ambulance to a local hospital, is treated, and survives. Suppose the hospital and

ambulance service protect the patient's identity as recommended by Nagel. However, the hospital also follows Nagel's instructions and leaves the date of incident, patient gender, severity of the incident and medical prognosis all unencrypted. This information has a legitimate purpose for statistical studies in medical research. Next, suppose that, at a later time, the person applies for a new job and the prospective employer wants to hire only persons who will maintain a low premium for the company's healthcare plan. It is technically possible for the employer to obtain this data from a service offering background checks. Once in possession of the person's report of hospitalization and the medical prognosis, the employer concludes that such a person will have on-going medical expenses. Therefore, the employer sends the person a polite rejection letter whatever their qualifications for employment may be.

The outcome is highly unfavorable for the former hospital patient and the outcome contradicts the purpose of the hospital's encryption. How could it happen? The service who revealed the information practices data mining, a technical process that has become a major industry serving business, advertising, and on-line databases. The service matches hospital records with ambulance records based on date, hospital name and patient gender. From the match for the unlucky person in this example, the service obtains the address where the medical emergency occurred. Then from real estate tax records, the service obtains the name of the individual residing at the address. Now the name of the person is connected to home address and medical prognosis. Modern computers make it possible to continuously produce such data for all individuals. Search firms practice data mining, store comprehensive results in inexpensive proprietary databases and sell the data to clients such as the employer in this example.

Although the teaching of Nagel on the subject of partial encryption is well meaning, it does not offer adequate privacy protections for today's needs. In contrast, the current invention fully conceals the data words on which data mining is practiced. The word "partial" in Applicant's invention refers to the feature of the new invention that leaves unencrypted only those words needed to characterize the syntax of a statement.

The multi-step negotiation protocol is designed to prevent indiscriminate downloading of encrypted information that is possible with Nagel's scheme. In the current Invention, only selected matches are delivered from one database to another and then only with the mutual concurrence of both parties.

Appendix 2: Sets of Interests Cannot Represent Value Ranges

Generally speaking, a subset of Snapp's methods is closely related to the methods of De Vries. As evidence, consider Snapp's stated purpose in his Abstract "encode a list so users of the list may make inquires to the coded list without the entire content of the list being revealed to users." This purpose echoes the statement in De Vries's Abstract "disclosure of at least one common interest between at least two entities while keeping non-common interests undisclosed or secret". Thus both De Vries and Snapp are working with lists where list membership is either true or false as represented by a bit string of at least one bit. By referencing these methods in connection with Claim 14, the Examiner draws the inference that they offer a method for concealing and then comparing range values. The inferred method is not the method disclosed by Applicant but let us take the suggestion and see where it leads.

If a person were to follow the methods of De Vries or Snapp and attempt to encode a range of values as a list, it would be necessary to encode a numerical range by making a list of every numerical value in the range and then encoding every value as one bit. If a bit is set, a value is in the range. If a bit is not set, the value is out of the range. A range may then be encoded by creating a bit string of length equal in length to the size of the set of all numerical values. To conceal the range value represented in such a bit string one might permute the bit string by some secret method. This required step is missing from both De Vries and Snapp, but let us assume a permutation method is provided somehow. Then, given two such encoded ranges concealed by permutation of order, one could search for and find any overlap in the ranges by determining the intersection where intersection is defined as the logical AND operation applied at every

bit position. From the result of bit string intersection, one may conclude that the original range values overlap if any bit is set in the result. If no bit is set, then the ranges do not overlap.

The process just described is the only one that appears compatible with the art cited by the Examiner. The Applicant would like to point out that he has offered a different method that is both novel and useful. If any person attempts to use the art cited by the Examiner for the purpose of the range value comparisons, it becomes clear quickly that the teaching of De Vries and Snapp as applied in this manner is impractical in consideration of the following analysis.

Suppose the numbers are represented by the C-language "long" type. A numerical range is represented as a pair of such values where one value is the minimum value of the range and the other is the maximum value. The C-language "long" type has 2 raised to the power 32 values. If the scheme attributed to Nagel were applied to range values, a numerical value range would be represented by a bit string of length 2 raised to the power 32 bits or 2 raised to the power 24 bytes or roughly 16 MB. Such large bit strings are very inefficient on current hardware. This is not a good method. Neither the Applicant nor Snapp recommends this method. De Vries is able to recommend it only because he hasn't considered its practicality. Thus we see that prior art does not lead in the direction of the novel method of Claim 14.

Appendix 3: De Vries and Similar Proposals Are Vulnerable to Dictionary Attack

Any person following the methods disclosed by De Vries's proposed solution is lead down a path to an insecure system that is vulnerable to a "Dictionary Attack" by any one of the parties in De Vries's system. To observe this insecurity, please note that De Vries specifies a system in which each party possesses a machine, which he describes in considerable detail. Each machine in the system uses the same identical encryption key to encrypt a party's "interests". Each machine then broadcasts the encrypted interests to all other machines. At this point, De Vries appears to forget that each machine has the encryption key. With this key, it is a simple manner for any of the parties to encrypt the full list of possible interests - thereby producing a dictionary that maps each encrypted term to its unencrypted form. Any party can then obtain another party's interest set by comparison of encrypted values with the full list.